Appendix III
TO OMB CIRCULAR NO. A-130

SECURITY OF FEDERAL AUTOMATED INFORMATION

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

2. Definitions

The term:

a. "adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

b. "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. "general support system" or "system" means an interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

d. "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. *Note*: All Federal information requires some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. Automated Information Security Programs. Agencies should implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program should implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM).

Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives.

At a minimum, agency programs should include the following controls in their general support systems and major applications:

a. Controls for general support systems.

1) Assign Responsibility for Security. Assign responsibility for security in each system to an official knowledgeable in the information technology used in the system and in providing security for such technology.

2) System Security Plan. Plan for the security of each general support system as part of the organization's information resources management (IRM) planning process.

The security plan should be consistent with guidance issued by the National Institute of Standards and Technology (NIST).

Independent advice and comment on the security plan should be solicited prior to the plan's implementation.

A summary of the security plans should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular.

Security plans should include:

a) Rules of the System. Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for the system. The rules should be based on the needs of the various users of the system. The security required by the rules should be only as stringent as necessary to provide adequate security for information in the system. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should also include appropriate limits on interconnections to other systems and should define service provision and restoration priorities. Finally, they should be clear about the consequences of behavior not consistent with the rules.

b) Awareness and Training. Ensure that all individuals are aware of their security responsibilities and trained how to fulfill them before allowing them access to the system.

Such awareness and training should assure that individuals are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise individuals about available assistance and technical security products and techniques.

Behavior consistent with the rules of the system and periodic refresher training should be required for continued access to the system.

c) Personnel Controls. Screen all individuals who are authorized to bypass technical and operational security controls of the system (e.g., LAN administrators or system programmers) commensurate with the risk and magnitude of loss or harm they could cause. Such screening should occur prior to the individuals' being authorized to bypass controls and periodically thereafter.

d) Incident Response Capability. Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.

This capability should coordinate with those in other organizations and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

e) Continuity of Support. Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

f) Technical Security. Ensure that cost-effective security products and techniques are appropriately used within the system.

g) System Interconnection. Obtain written management authorization based upon the acceptance of risk to the system prior to connecting with other systems.

Where connection is authorized, controls should be established which are consistent with the rules of the system and in accordance with guidance from NIST.

3) Review of Security Controls. Periodically review the security controls in each system commensurate with the acceptable level of risk for the system established in its rules, especially when significant modifications are made and at least every 3 years.

Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan or no authorization to process in a system.

4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system.

Use of the system should be re-authorized at least every three years.

b. Controls for Major Applications.

1) Assign Responsibility for Security. Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information processed by the application and in the management, operational, and technical controls used to protect it.

This official should assure that effective security products and techniques are appropriately used in the application and should be contacted when a security incident occurs concerning the application.

2) Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate.

The plan should be consistent with guidance issued by NIST.

Advice and comment on the plan should be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation.

A summary of the security plans should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act.

Application security plans should include:

a) Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules should be as stringent as necessary to provide adequate security for the application and the information in it. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules should be clear about the consequences of behavior not consistent with the rules.

b) Specialized Awareness and Training. Before allowing individuals access to the application, ensure that all individuals receive specialized awareness and training focused on their responsibilities and the application rules.

This may be in addition to the awareness and training required for access to a system. Such awareness and training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high risk application).

c) Personnel Security. Incorporate controls such as separation of duties, least privilege and individual accountability into the application as appropriate.

In cases where such controls cannot adequately protect the application and information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening should be done prior to the individuals being authorized to access the application and periodically thereafter.

d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls. Ensure that appropriate security controls are specified, designed into, tested, and accepted in accordance with guidance issued by NIST.

f) Information Sharing. Ensure that information shared from the application is protected appropriately, relative to the protection provided when information is within the application.

g) Public Access Controls. Where an agency's application promotes or permits public access, additional security controls should be added to protect the integrity of the application and the confidence the public has in the application. Such controls should include segregating information made directly accessible to the public from official agency records (e.g., by putting information onto a bulletin board).

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years.

Consider identifying a deficiency pursuant to the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application.

Results of the most recent review or audit of controls should be a factor in management authorizations.

The application should be authorized prior to operating and re-authorized at least every three years thereafter.

Management authorization implies accepting the risk of each system used by the application.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce should:

1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

4) Provide guidance and assistance, as appropriate, to agencies concerning effective controls when interconnecting with other systems.

5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

b. Security Policy Board. The Security Policy Board should:

1) Act, in accordance with applicable national security directives, to coordinate the security activities of the Federal government regarding the security of automated information systems that process national security information.

c. Department of Defense. The Secretary of Defense should:

1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

d. Office of Personnel Management. The Director of the Office of Personnel Management should:

1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

e. General Services Administration. The Administrator of General Services should:

1) Assure that the Federal Information Resources Management Regulation provides guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended)

2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services contract).

3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

f. Department of Justice. The Attorney General should:

1) Provide guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents.

2) Pursue appropriate legal actions when security incidents occur.

5. Correction of Deficiencies and Reports

a. Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. Reports on Deficiencies. In accordance with OMB Circular No. A-123, if a deficiency control is judged by the agency head to be material when weighed against other agency deficiencies, it should be included in the annual FMFIA report.

Less significant deficiencies should be reported and progress on corrective actions tracked at the appropriate agency level.

c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the five-year plan required by the Paperwork Reduction Act (44 U.S.C. 3505).